UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

AARON RAHMAN, *individually and on behalf of all others similarly situated*, Plaintiff, v. COINBASE, INC. and COINBASE GLOBAL, INC., Defendants.	No. _____ **JURY TRIAL DEMANDED**

CLASS ACTION COMPLAINT FOR DAMAGES

Plaintiff Aaron Rahman ("Plaintiff"), individually and on behalf of all others similarly situated ("Class Members"), brings this action against Defendants Coinbase, Inc. and Coinbase Global, Inc. (collectively, "Defendants" or "Coinbase") and alleges, upon personal knowledge as to his own actions and his counsel's investigation, and upon information and belief as to all other matters, as follows:

INTRODUCTION

1. Plaintiff brings this class action against Defendants for their failure to properly secure and safeguard the personally identifiable information ("PII") of Plaintiff and other similarly situated individuals ("Class Members").

2. On May 15, 2025, Defendants announced on their website that an unnamed threat actor gained access to Defendant's information systems through a cybersecurity incident, involving information about certain Coinbase customer accounts, as well as internal Coinbase documentation, including materials relating to customer-service and account-management

systems.[1]

3. On May 11, 2025, Defendants received email communications from an unknown threat actor claiming to have obtained information through Coinbase's contractors or employees working in support roles outside of the United States.[2] This resulted in a double-extortion ransomware attack on its systems in which hackers infiltrated Defendant's information systems, performed reconnaissance operations, identified and stole valuable files containing Class Members' PII, and then encrypted Defendant's systems.

4. Before Defendants discovered the systems interruption, the hackers had already been in Defendants' information systems and downloaded files.

5. Given that Defendants did not realize that it had been infiltrated until the hackers announced themselves by disrupting Defendants' information systems, it is likely that Defendants failed to implement necessary and expected monitoring, alerting, and data loss prevention tools that would have identified the malicious activity in a timelier manner.

6. Because of Defendants' failures, Plaintiff and the proposed Class Members have suffered a severe invasion of their privacy and must now face a substantial increase in identity theft and financial fraud for years to come.

PARTIES

7. Plaintiff Aaron Rahman is a resident and citizen of Mt. Vernon, New York.

8. Defendant Coinbase, Inc. is a Delaware corporation with its principal executive offices located at One Madison Avenue, Suite 2400, New York, New York 10016.[3]

---

[1] *See* http://www.sec.gov/Archives/edgar/data/1679788/000167978825000094/coin-20250514.htm#:~:text=On%20May%2011%2C%202025%2C%20Coinbase%2C%20Inc.
[2] *Id*.
[3] *See* http://s27.q4cdn.com/397450999/files/doc_events/2024/Oct/30/Coinbase-Global-Inc-Q3-2024-10Q.pdf

9. Defendant Coinbase Global, Inc., the parent company of Coinbase, Inc., is a Delaware corporation with its principal executive offices located at One Madison Avenue, Suite 2400, New York, New York 10016.[4]

JURISDICTION AND VENUE

10. The Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1332(d). The amount of controversy exceeds the sum or value of $5,000,000 exclusive of interests and costs, there are more than 100 putative Class members, and minimal diversity exists because one or more putative Class members are citizens of a different state than Defendants.

11. This Court has personal jurisdiction over Defendants because they maintain their principal place of business and operations in the state of New York and because Defendants intentionally availed themselves of this jurisdiction by providing services in the state of New York.

12. Venue is proper in the Court pursuant to 28 U.S.C. § 1391 because Defendants' principal place of business is in this District, Defendants operate in this District, and a substantial portion of the events, acts, and omissions giving rise to Plaintiff's claims occurred in this District.

FACTUAL ALLEGATIONS

A. Defendants Provide Cryptocurrency Exchange Services Involving Highly Sensitive Data.

13. Defendants operate a cryptocurrency exchange with a quarterly trading volume of $393 billion.[5]

14. As part of their business, Defendants collected the PII of Plaintiff and the proposed Class Members, which it held and continues to hold unencrypted in its information systems.

[4] *See id*.
[5] *See* http://www.coinbase.com/about

15. Defendants advertise themselves as "the most trusted place for people and businesses to buy, sell, and use crypto." [6]

16. Defendants allow their customers to trade cryptocurrency by providing a "trusted platform that makes it easy for people and institutions to engage with crypto assets, including trading, staking, safekeeping, spending, and fast, free global transfers." [7]

17. Defendants made promises and representations to Plaintiff and Class Members that his PII would be kept safe and confidential, and that the privacy of that information would be maintained.

18. Plaintiff's and Class Members' PII was provided to Defendants with the reasonable expectation and on the mutual understanding that Defendants would comply with its obligations to keep such information confidential and secure from unauthorized access.

19. Defendants had a duty to adopt reasonable measures to protect the PII of Plaintiff and Class Members from involuntary disclosure to third parties. Defendants have a legal duty to keep consumer's PII safe and confidential.

20. Defendants had obligations created by the Federal Trade Commission Act, 15 U.S.C. § 45 ("FTCA"), industry standards, and representations made to Plaintiff and Class Members, to keep his PII confidential and to protect it from unauthorized access and disclosure.

21. By obtaining, collecting, using, and deriving a benefit from Plaintiff's and Class Members' PII, Defendants assumed legal and equitable duties and knew or should have known it was responsible for protecting Plaintiff's and Class Members' PII from disclosure.

[6] *See* http://www.coinbase.com/
[7] *See* http://www.coinbase.com/about

B. The Data Breach

22. As previously stated, on May 11, 2025, Defendants received an email communication from an unknown threat actor claiming to have obtained information about certain Coinbase customer accounts, as well as internal Coinbase documentation, including materials relating to customer-service and account-management systems. [8]

23. A threat actor reportedly targeted Coinbase's customer support agents overseas and used cash offers to convince a group of insiders to copy data in their customer support tools for less than 1% of Coinbase monthly transacting users with the goal of gathering a customer list they could contact while pretending to be Coinbase- tricking people into handing over their crypto.

24. The unknown threat actor demanded $20 million in exchange for not publicly disclosing the information. Defendants said they would not pay.[9]

25. The stolen information includes names, addresses, email addresses, the last four digits of Social Security numbers, masked bank-account numbers and some bank account identifiers, Government-ID images (*e.g.,* driver's license, passport), account data (balance snapshots and transaction history), and limited corporate data (including documents, training material, and communications available to support agents).[10]

26. On May 15, 2025, Defendants reported the Data Breach on their website.[11]

Defendants' Data Breach Was Imminently Foreseeable

27. Defendants' data security obligations were particularly important given the substantial increase in cyberattacks and/or data breaches targeting institutions that collect and store

[8] *See* http://www.sec.gov/Archives/edgar/data/1679788/000167978825000094/coin-20250514.htm#:~:text=On%20May%2011%2C%202025%2C%20Coinbase%2C%20Inc.
[9] *See* http://www.coinbase.com/blog/protecting-our-customers-standing-up-to-extortionists
[10] *Id*.
[11] *Id*.

PII, like Defendants, preceding the date of the Data Breach.

28. Data thieves regularly target institutions like Defendants due to the highly sensitive information in his custody. Defendants knew and understood that unprotected PII is valuable and highly sought after by criminal parties who seek to illegally monetize that PII through unauthorized access.

29. In 2021, a record 1,862 data breaches occurred, resulting in approximately 293,927,708 sensitive records being exposed, a 68% increase from 2020.[12]

30. As a custodian of PII, Defendants knew, or should have known, the importance of safeguarding the PII entrusted to it by Plaintiff and Class Members, and of the foreseeable consequences if its data security systems were breached, including the significant costs imposed on Plaintiff and Class Members because of a breach.

31. Despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

32. Defendants were, or should have been, fully aware of the unique type and the significant volume of data in its systems, amounting to potentially thousands of individuals' detailed PII, and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

33. The injuries to Plaintiff and Class Members were directly and proximately caused by Defendants' failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

[12] *See* Identity Theft Res. Ctr., *2021 Data Breach Annual Report*, at 6 (Jan. 2022), https://notified.idtheftcenter.org/s/.

34. The ramifications of Defendants' failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen, fraudulent use of that information and damage to victims may continue for years.

Value of Personally Identifiable Information

35. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[13] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[14]

36. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[15]

37. For example, PII can be sold at a price ranging from $40 to $200.[16] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[17]

38. Based on the foregoing, the information compromised in the Data Breach is even

[13] 17 C.F.R. § 248.201 (2013).
[14] *Id.*
[15] Anita George, *Your Personal Data Is for Sale on The Dark Web. Here's How Much It Costs,* DIGITAL TRENDS (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs.
[16] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web.
[17] *In the Dark*, VPNOVERVIEW, 2019, https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark.

more significant because it includes Social Security numbers and other government identification, which is significantly difficult if not impossible to change.

39. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information . . . [is] worth more than 10x on the black market."[18]

40. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[19]

Defendants Failed to Comply with FTC Guidelines

41. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the FTCA, 15 U.S.C. § 45. *See, e.g.*, *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

42. In October 2016, the FTC updated its publication, Protecting Personal Information:

---

[18] Tim Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, (Feb. 6, 2015), https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html.

[19] *Report to Congressional Requesters*, GAO, at 29 (June 2007), https://www.gao.gov/assets/gao-07-737.pdf.

A Guide for Business, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal consumer information they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand his network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack into the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.

43. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor the network for suspicious activity, and verify that third-party service providers have implemented reasonable security measures.

44. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data by treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by the FTC Act. Orders resulting from these actions further clarify the measures businesses must take to meet his data security obligations.

45. As evidenced by the Data Breach, Defendants failed to properly implement basic data security practices and failed to audit, monitor, or ensure the integrity of its data security practices, or to appropriately prepare to face a data breach and respond to it in a timely manner. Defendants' failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff's and Class Members' PII constitutes an unfair act or practice prohibited by

Section 5 of the FTC Act.

46. Defendants were at all times fully aware of its obligation to protect the PII of consumers under the FTC Act yet failed to comply with such obligations. Defendants were also aware of the significant repercussions that would result from their failure to do so. Accordingly, Defendants' conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

Defendants Failed to Comply with Industry Standards.

47. Experts studying cybersecurity routinely identify institutions that store PII like Defendants as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

48. Some industry best practices that should be implemented by institutions dealing with sensitive PII, like Defendants, include, but are not limited to: educating all employees, strong password requirements, multilayer security including firewalls, anti-virus and anti-malware software, encryption, multi-factor authentication, backing up data, implementing reasonable systems to identify malicious activity, implementing reasonable governing policies, and limiting which employees can access sensitive data. As evidenced by the Data Breach and its timeline, Defendants failed to follow some or all these industry best practices.

49. Other best cybersecurity practices that are standard at large institutions that store PII include: installing appropriate malware detection software; monitoring and limiting network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches, and routers; monitoring and protecting physical security systems; and training staff regarding these points.

50. Moreover, a properly trained helpdesk that understands how to face social engineering attacks is an expected part of all cybersecurity programs.

51. Defendants failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 2.0 (including without limitation PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

52. Defendants failed to comply with these accepted standards, thereby permitting the Data Breach to occur.

Common Injuries & Damages

53. Because of Defendants' ineffective and inadequate data security practices, the Data Breach, and the foreseeable consequences of PII ending up in the possession of criminals, the risk of identity theft to the Plaintiff and Class Members has materialized and is imminent, and Plaintiff and Class Members have all sustained actual injuries and damages, including: (a) invasion of privacy; (b) loss of time and loss of productivity incurred mitigating the materialized risk and imminent threat of identity theft risk; (c) the loss of benefit of the bargain (price premium damages); and (d) the continued risk to his PII, which remains in the possession of Defendants, and which is subject to further breaches, so long as Defendants fail to undertake appropriate and adequate measures to protect Plaintiff's and Class Members' PII.

The Data Breach Increases Victims' Risk of Identity Theft.

54. Plaintiff and Class Members are at a heightened risk of identity theft for years to come, especially because Defendants' failures resulted in Plaintiff's and Class Members' Social

Security number falling into the hands of identity thieves.

55. The unencrypted PII of Class Members has already or will end up for sale on the dark web because that is the *modus operandi* of hackers. Indeed, when these criminals do not post the data to the dark web, it is usually at least sold on private Telegram channels to even further identity thieves who purchase the PII for the express purpose of conducting financial fraud and identity theft operations.

56. Further, the standard operating procedure for cybercriminals is to use some data, like the Social Security numbers here, to access "fullz packages" of that person to gain access to the full suite of additional PII that those cybercriminals have access through other means. Using this technique, identity thieves piece together full pictures of victim's information to perpetrate even more types of attacks.[20]

57. With "Fullz" packages, cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy to assemble complete dossiers on individuals.

58. The development of "Fullz" packages means here that the stolen PII from the Data

[20] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, social security number, date of birth, and more. As a rule of thumb, the more information you have on a victim, the more money that can be made off those credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen from Texas Life Insurance Firm*, Krebs on Security (Sep. 18, 2014), https://krebsonsecuritv.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm.

Breach can easily be used to link and identify it to Plaintiff's and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

Loss of Time to Mitigate Risk of Identity Theft and Fraud

59. Because of the recognized risk of identity theft, when a data breach occurs, and an individual is notified by a company that his PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm and Defendants arguing that the individual failed to mitigate damages.

60. The need to spend time mitigating the risk of harm is especially important in cases like this where Plaintiff's and Class Members' Social Security numbers or other government identification are affected.

61. By spending this time, data breach Plaintiff was not manufacturing his own harm, he was taking necessary steps at Defendants' direction and because the Data Breach included his Social Security number.

62. Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions to remedy the harms they have or may experience because of the Data Breach, such as contacting credit bureaus to place freezes on his accounts; changing passwords and re-securing his own computer networks; and checking his financial accounts and

health insurance statements for any indication of fraudulent activity, which may take years to detect.

63. These efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to his good name and credit record."[21]

The Future Cost of Credit and Identity Theft Monitoring Is Reasonable and Necessary

64. Based on the value of the information stolen, the data either has or will be sold to cybercriminals whose mission it is to perpetrate identity theft and fraud. Even if the data is not posted online, these data are ordinarily sold and transferred through private Telegram channels wherein thousands of cybercriminals participate in a market for such data so that they can misuse it and earn money from financial fraud and identity theft of data breach victims.

65. Such fraud may go undetected for years; consequently, Plaintiff and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

66. The retail cost of credit monitoring and identity theft monitoring can cost $200 or more per year per Class Member. This is a reasonable and necessary cost to monitor and protect Class Members from the risk of identity theft that arose from the Data Breach. This is a future cost for a minimum of seven years that Plaintiff and Class Members would not need to bear but for Defendants' failure to safeguard his PII.

Plaintiff's Experience

67. Plaintiff is a current customer of Defendants and exchanges cryptocurrency on their

[21] *See* U.S. Gov't Office, GAO-07-737, *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), https://www.gao.gov/new.items/d07737.pdf.

platform.

68. Thus, at the time of the Data Breach, Defendants retained Plaintiff's PII in its system.

69. Plaintiff's PII was compromised in the Data Breach and stolen by identity thieves who illegally accessed Defendants' network for the specific purpose of targeting the PII.

70. Plaintiff has started receiving spam text messages relating to his Coinbase account.

71. Plaintiff takes reasonable measures to protect his PII.

72. Plaintiff suffered actual injury in the form of a severe privacy invasion because of his PII, including his Social Security number and driver's license, falling into the hands of identity thieves whose mission it is to use that information to perpetrate identity theft and financial fraud.

73. Plaintiff suffered lost time, interference, and inconvenience because of the Data Breach and has experienced stress and anxiety due to increased concerns for the loss of his privacy and because he knows he must now face a substantial increase in identity theft and financial fraud attempts for years to come.

74. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII, especially his name and Social Security number, being placed in the hands of criminals whose mission it is to misuse that data.

75. Defendants obtained and continues to maintain Plaintiff's PII and has a continuing legal duty and obligation to protect that PII from unauthorized access and disclosure. Plaintiff's PII was compromised and disclosed because of the Data Breach.

76. Because of the Data Breach, Plaintiff anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach.

77. Because of the Data Breach, Plaintiff is at a present risk and will continue to be at increased risk of identity theft and fraud for years to come, in addition to the significantly increased risk of identity theft and financial fraud that Plaintiff must now face because of Defendants' failures.

78. As a result of the Data Breach, Plaintiff has experienced a significant invasion of his privacy which has caused him to experience significant anxiety, depression, and fear.

CLASS ALLEGATIONS

79. Plaintiff brings this class action on behalf of himself and on behalf of all others similarly situated pursuant to Rule 23(b)(2) and 23(b)(3) of the Federal Rules of Civil Procedure.

80. The Class that Plaintiff seeks to represent is defined as follows:

> All persons whose PII was compromised during the Data Breach that occurred at Defendant in or about May 11, 2025 (the "Class").

81. Excluded from the Class is the following individuals and/or entities: Defendants and Defendants' parents, subsidiaries, affiliates, officers and directors, and any entity in which a Defendant has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

82. Plaintiff reserves the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate should discovery reveal that the class should include further categories of individuals.

83. This action is brought and may be maintained as a class action because there is a well-defined community of interest among many persons who comprise a readily ascertainable

class. A well-defined community of interest exists to warrant class-wide relief because Plaintiff and all members of the Class were subjected to the same wrongful practices by Defendants, entitling them to the same relief.

84. The Class is so numerous that individual joinder of its members is impracticable.

85. Common questions of law and fact exist as to members of the Class and predominate over any questions which affect only individual members of the Class. These common questions include, but are not limited to:

a. Whether and to what extent Defendants had a duty to protect the PII of Plaintiff and Class Members;

b. Whether Defendants had a duty not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;

c. Whether Defendants had a duty not to use the PII of Plaintiff and Class Members for non-business purposes;

d. Whether Defendants failed to adequately safeguard the PII of Plaintiff and Class Members;

e. When Defendants actually learned of the Data Breach;

f. Whether Defendants adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;

g. Whether Defendants violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;

h. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class Members;

k. Whether Plaintiff and Class Members are entitled to actual, damages, and/or statutory damages as a result of Defendants' wrongful conduct;

l. Whether Plaintiff and Class Members are entitled to restitution because of Defendants' wrongful conduct; and

m. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced because of the Data Breach.

86. Plaintiff is a member of the Class he seeks to represent, and his claims and injuries are typical of the claims and injuries of the other Class Members.

87. Plaintiff will adequately and fairly protect the interests of other Class Members. Plaintiff has no interests adverse to the interests of absent Class Members. Plaintiff is represented by legal counsel with substantial experience in class action litigation. The interests of Class Members will be fairly and adequately protected by Plaintiff and his counsel.

88. Defendants have acted or refused to act on grounds that apply generally to the Class Members, so that final injunctive relief or corresponding declaratory relief is appropriate respecting the Class as a whole.

89. A class action is superior to other available means for fair and efficient adjudication of the claims of the Class and would be beneficial for the parties and the court. Class action treatment will allow a large number of similarly situated persons to prosecute their common claims

in a single forum, simultaneously, efficiently, and without the unnecessary duplication of effort and expense that numerous individual actions would require. The amounts owed to the many individual Class Members are likely to be relatively small, and the burden and expense of individual litigation would make it difficult or impossible for individual members of the class to seek and obtain relief. A class action will serve an important public interest by permitting such individuals to effectively pursue recovery of the sums owed to them. Further, class litigation prevents the potential for inconsistent or contradictory judgments raised by individual litigation. Plaintiff is unaware of any difficulties that are likely to be encountered in the management of this action that would preclude its maintenance as a class action.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

90. Plaintiff and the Class re-allege and incorporate all the above allegations.

91. Plaintiff and the Class provided and entrusted Defendants with certain PII as a condition of their employment based upon the premise and with the understanding that Defendants would safeguard their information, use their PII for business purposes only, and/or not disclose their PII to unauthorized third parties.

92. Defendants have full knowledge of the sensitivity of the PII and the types of harm that Plaintiff and the Class could and would suffer if the PII were wrongfully disclosed.

93. Defendants knew or reasonably should have known that the failure to exercise due care in the collecting, storing, and using of the PII of Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the Class, even if the harm occurred through the criminal acts of a third party, which were eminently foreseeable given the ubiquity of data breaches.

94. Defendants had a duty to exercise reasonable care in overseeing, safeguarding,

securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendants' security protocols to ensure that the PII of Plaintiff and the Class in Defendants' possession was adequately secured and protected.

95. Defendants owed a duty to Plaintiff and the Class to implement intrusion detection processes that would detect a data breach or unauthorized access to its systems in a timely manner.

96. Defendants also had a duty to exercise appropriate clearinghouse practices to remove PII it was no longer required to retain pursuant to regulations, including that of former employees.

97. Defendants also had a duty to employ proper procedures to detect and prevent the improper access, misuse, acquisition, and/or dissemination of the PII of Plaintiff and the Class.

98. Defendants' duty to use reasonable security measures arose because of the special relationship that existed between both Defendants and Plaintiff and the Class. That special relationship arose because Plaintiff and the Class entrusted Defendants with their confidential PII, a necessary part of their relationship with Defendants.

99. Defendants owed a duty to disclose the material fact that Defendants' data security practices were inadequate to safeguard the PII of Plaintiff and the Class.

100. A breach of security, unauthorized access, and resulting injury to Plaintiff and the Class was reasonably foreseeable, particularly considering Defendants' inadequate security practices.

101. Plaintiff and the Class were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the PII of Plaintiff and the Class, the critical importance of providing

adequate security of that PII, and the necessity for encrypting PII stored on Defendants' system.

102. Defendants' own conduct created a foreseeable risk of harm to Plaintiff and the Class. Defendants' misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendants' misconduct also included its decisions not to comply with industry standards for the safekeeping of the PII of Plaintiff and the Class, including basic encryption techniques freely available to Defendants.

103. Plaintiff and the Class had no ability to protect their PII that was in, and likely remains in, Defendants' possession.

104. Defendants had and continues to have a duty to adequately disclose that the PII of Plaintiff and the Class within Defendants' possession, how it was compromised, and precisely the types of data that was compromised and when. Such notice was necessary to allow Plaintiff and the Class to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII by third parties.

105. Defendants have admitted that the PII of Plaintiff and the Class was wrongfully accessed, acquired, and/or released to unauthorized third persons because of the Data Breach.

106. Defendants, through their actions and/or omissions, unlawfully breached its duties to Plaintiff and the Class by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII of Plaintiff and the Class during the time the PII was within Defendants' possession or control.

107. Defendants improperly and inadequately safeguarded the PII of each Plaintiff and the Class in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

108. Defendants failed to heed industry warnings and alerts to provide adequate

safeguards to protect the Plaintiff and the Class in the face of increased risk of theft.

109. Defendants, through their actions and/or omissions, unlawfully breached its duty to Plaintiff and the Class by failing to have appropriate procedures in place to detect unauthorized access or intrusions and prevent dissemination of their PII. Additionally, Defendants failed to disclose to Plaintiff and the Class that Defendants' security practices were inadequate to safeguard the PII of Plaintiff and the Class.

110. Defendants breached their duty to exercise appropriate clearinghouse practices by failing to remove PII it was no longer required to retain pursuant to regulations, including PII of former patients.

111. Defendants, through their actions and/or omissions, unlawfully breached their duty to adequately and timely disclose to Plaintiff and the Class the existence and scope of the Data Breach.

112. But for Defendants' wrongful and negligent breach of duties owed to Plaintiff and the Class, the PII of Plaintiff and the Class would not have been compromised.

113. There is a close causal connection between Defendants' failure to implement security measures to protect the PII of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by each Plaintiff and the Class. The PII of Plaintiff and the Class was accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such PII by adopting, implementing, and maintaining appropriate security measures and oversight.

114. As a direct and proximate result of Defendants' negligence, Plaintiff and the Class have suffered and will continue to suffer injury.

115. Additionally, as a direct and proximate result of Defendants' negligence, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PII which

remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII in its continued possession.

116. As a direct and proximate result of Defendants' negligence, Plaintiff and the Class are entitled to and demand actual, consequential, and nominal damages.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiff and the Class)

117. Plaintiff and the Class re-allege and incorporate all the above allegations.

118. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

119. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiff and the Class.

120. Defendants violation of Section 5 of the FTC Act constitutes negligence *per se*.

121. Plaintiff and the Class are within the class of persons that the FTC Act was intended to protect.

122. The harm that occurred because of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, because of their failure to employ reasonable data security measures and avoid unfair and

deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

123. As a direct and proximate result of Defendants' negligence *per se*, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity of how their PII is used; iii) the compromise, publication, and/or theft of their PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII, which remain in Defendants' possession and are subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect the PII of Plaintiff and the Class; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Personal Information compromised as a result of the Data Breach for the remainder of the lives of Plaintiff and the Class.

COUNT III
Breach of Implied Contract
(On Behalf of Plaintiff and the Class)

124. Plaintiff and the Class re-allege and incorporate all the above allegations.

125. Defendants required Plaintiff and the Class to provide and entrust their PII as a condition of his employment.

126. Plaintiff and the Class paid money to Defendants in exchange for services, as well as Defendants' promises to protect their PII from unauthorized disclosure.

127. Defendants implicitly promised to implement reasonable, industry standard

cybersecurity measures and to make sure that Plaintiff and Class Members' PII would remain reasonably protected.

128. As a condition of his employment with Defendants, Plaintiff and the Class provided and entrusted their PII. In so doing, Plaintiff the Class entered into implied contracts with Defendants by which Defendants agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

129. A meeting of the minds occurred, as Plaintiff and Class Members agreed, *inter alia*, to provide accurate and complete PII and to pay Defendants in exchange for Defendants' collective agreement to, *inter alia*, protect their PII.

130. Plaintiff and Class Members would not have entrusted their PII to Defendants in the absence of Defendants' implied promise to adequately safeguard this confidential personal and medical information.

131. Plaintiff and the Class fully performed their obligations under the implied contracts with Defendants.

132. Defendants have breached the implied contracts it made with Plaintiff and the Class by making their PII accessible from the internet (regardless of any mistaken belief that the information was protected) and failing to make reasonable efforts to use the latest security technologies designed to help ensure that the PII was secure, failing to encrypt Plaintiff and Class Members' PII, failing to safeguard and protect their PII, and by failing to provide timely and accurate notice to them that PII was compromised as a result of the data breach.

133. Defendants' failure to meet their promises constitute breach of the implied contracts.

134. Because Defendants allowed unauthorized access to Plaintiff and Class Members' PII and failed to safeguard the PII, Defendants breached their contracts with Plaintiff and Class Members.

135. Defendants breached their contracts by not meeting the minimum level of protection of Plaintiff and Class Members' protected health information and other PII, because Defendants did not prevent against the Data Breach.

136. As a direct and proximate result of Defendants' above-described breach of implied contract, Plaintiff and the Class are now subject to the present and continuing risk of fraud, and are suffering (and will continue to suffer) the ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

137. As a result of Defendants' breach of implied contract, Plaintiff and the Class are entitled to and demand actual, consequential, and nominal damages.

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

138. Plaintiff and the Class re-allege and incorporate all the above allegations.

139. This Count is pled in the alternative to Count III, Breach of Implied Contract.

140. Plaintiff and the Class conferred a benefit upon Defendants in providing PII to

Defendants.

141. Defendants appreciated or had knowledge of the benefits conferred upon it by Plaintiff and the Class. Defendants also benefited from the receipt of Plaintiff's and the Class's PII, as this was used to facilitate its services to Plaintiff and the Class.

142. Defendants enriched themselves by saving the costs it reasonably should have expended on data security measures to secure Plaintiff's and Class Members' PII.

143. Instead of providing a reasonable level of security, or retention policies, which would have prevented the Data Breach, Defendants instead calculated to avoid its data security obligations at the expense of Plaintiff and the Class by utilizing cheaper, ineffective security measures. Plaintiff and the Class, on the other hand, suffered as a direct and proximate result of Defendants' failure to provide the requisite security.

144. Under principles of equity and good conscience, Defendants should not be permitted to retain the full value of Plaintiff's and the Class's PII because Defendants failed to adequately protect it.

145. Plaintiff and the Class have no adequate remedy at law.

146. Defendants should be compelled to disgorge into a common fund for the benefit of Plaintiff and members of the Class all unlawful or inequitable proceeds received by them because of their misconduct and Data Breach.

COUNT V
Violation of New York General Business Law § 349
(On Behalf of Plaintiff and the Class)

147. Plaintiff and the Class re-allege and incorporate all the above allegations.

148. The New York General Business Law ("GBL") § 349 prohibits deceptive acts or practices in the conduct of any business, trade, or commerce, or in the furnishing of any service in

the state of New York.

149. By reason of the conduct alleged herein, Defendants has engaged in unlawful practices within the meaning of GBL § 349. The conduct alleged herein is a "business practice" within the meaning of GBL § 349, and the deception occurred within New York State.

150. Defendants stored Plaintiff's and Class Members' PII on the aforementioned information systems. Defendants knew or should have known it did not employ reasonable, industry standard, and appropriate security measures that complied "with federal regulations" and that would have kept Plaintiff's and Class Members' PII secure and prevented the loss or misuse of Plaintiff's and Class Members' PII. Further, Defendants knew or should have known that they each did not employ reasonable safeguards and oversight to ensure that Plaintiff's and Class Members' PII was protected.

151. Plaintiff and Class Members never would have provided their PII to Defendants if they had been told or knew that Defendants would fail to maintain sufficient security to keep such PII from being taken by others.

152. Defendants violated GBL § 349 by misrepresenting, both by affirmative conduct and by omission, the safety of Defendants' storage and services, specifically the security thereof, and its ability to safely store and dispose of Plaintiff's and Class Members' PII.

153. Defendants also violated GBL § 349 by failing to implement reasonable and appropriate security measures or follow industry standards for data security, and by failing to immediately notify Plaintiff and Class Members of the Data Breach. If Defendants had complied with these legal requirements, Plaintiff and Class Members would not have suffered the damages related to the Data Breach.

154. Defendants' practices, acts, policies, and course of conduct violate GBL § 349 in

that:

a. Defendants actively and knowingly misrepresented or omitted disclosure of material information to Plaintiff and Class Members at the time it provided such PII that Defendants did not have sufficient security or mechanisms to protect PII; and

b. Defendants failed to give timely warnings and notices regarding the defects and problems with the security of its computer systems to protect Plaintiff's and Class Members' PII. Defendants possessed actual knowledge of the inherent risks in inadequate data security.

155. Plaintiff and the Class were entitled to believe, and did believe, that Defendants would take appropriate measures to keep their PII safe. Defendants did not disclose that Plaintiff's and Class Members' PII was vulnerable to malicious actors, and Defendants were the only one in possession of that material information, which it had a duty to disclose.

156. The aforementioned conduct constitutes an unconscionable commercial practice in that Defendants have, by the use of false or deceptive statements and/or knowing intentional material omissions, misrepresented and/or concealed the inadequate nature of its security practices, resulting in the Data Breach.

157. Members of the public were deceived by Defendants' misrepresentations and failures to disclose.

158. Such acts by Defendants are and were deceptive acts or practices which are and/or were likely to mislead a reasonable consumer providing his PII to Defendants. Said deceptive acts and practices are material. The requests for and use of such PII in New York through deceptive means occurring in New York were consumer-oriented acts and thereby falls under the New York

consumer protection statute, GBL § 349.

159. Defendants' wrongful conduct caused Plaintiff and Class Members to suffer a consumer-related injury by causing them to incur substantial expense to protect from misuse of the PII by third parties and placing Plaintiff and Class Members at serious risk for monetary damages.

160. As a direct and proximate result of Defendants' violations of the above, Plaintiff and Class Members suffered damages including, but not limited to: unauthorized use of their PII; theft of their personal and financial information; costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts; damages arising from the inability to use their PII; costs associated with time spent and the loss of productivity or the enjoyment of one's life from taking time to address an attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, purchasing credit monitoring and identity theft protection services, initiating and monitoring credit freezes, and the stress, nuisance, and annoyance of dealing with all issues resulting from the Data Breach; the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals; damages to and diminution in value of their PII entrusted to Defendants; and the loss of Plaintiff's and Class Members' privacy.

161. In addition to or in lieu of actual damages, because of the injury, Plaintiff and the Class seek statutory damages for each injury and violation which has occurred.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff, on behalf of himself and Class Members, requests judgment against Defendants and that the Court grant the following:

A. For an Order certifying the Class, and appointing Plaintiff and his Counsel to

represent the Class;

B. For equitable relief enjoining Defendants from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of the PII of Plaintiff and Class Members, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiff and Class Members;

C. For injunctive relief requested by Plaintiff, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiff and Class Members, including but not limited to an order:

i. prohibiting Defendants from engaging in the wrongful and unlawful acts described herein;

ii. prohibiting Defendants from further deceptive practices and making untrue statements about the Data Breach and the stolen PII

iii. requiring Defendants to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state, or local laws;

iv. requiring Defendants to delete, destroy, and purge the personal identifying information of Plaintiff and Class Members unless Defendants can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiff and Class Members;

v. requiring Defendants to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the PII of Plaintiff and Class Members;

vi. requiring Defendants to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendants to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendants to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendants to segment data by, among other things, creating firewalls and access controls so that if one area of Defendants' network is compromised, hackers cannot gain access to other portions of Defendants' system;

x. requiring Defendants to conduct regular database scanning and securing checks;

xi. requiring Defendants to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring Defendants to routinely and continually conduct internal training

and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendants to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees' compliance with Defendants' policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendants to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendants' information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendants to meaningfully educate all Class Members about the threats that they face because of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals must take to protect themselves;

xvi. requiring Defendants to implement logging and monitoring programs sufficient to track traffic to and from Defendants' servers; and for a period of 10 years, appointing a qualified and independent third-party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendants' compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report

any deficiencies with compliance of the Court's final judgment;

D. For an award of damages, including actual, consequential, nominal, and statutory damages, as allowed by law in an amount to be determined;

E. For an award of restitution and damages in an amount to be determined;

F. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

G. For prejudgment interest on all amounts awarded; and

H. Such other and further relief as the Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff hereby demands that this matter be tried before a jury.

Dated: June 2, 2025

Respectfully submitted,

/s/ Steven P. Sukert

Steven P. Sukert, NY Bar No. 5690532
Jeff Ostrow (*pro hac vice* forthcoming)
KOPELOWITZ OSTROW, P.A.
1 West Las Olas Blvd., Suite 500
Fort Lauderdale, FL 33301
Tel.: (954) 332-4200
sukert@kolawyers.com
ostrow@kolawyers.com

Counsel for Plaintiff and the Putative Class